Załącznik Nr 1
do Uchwały Krajowej Rady Izby Architektów RP O-012-IV-2018
z dnia 23 maja 2018

POLITYKA BEZPIECZEŃSTWA INFORMACJI
Izby Architektów Rzeczypospolitej Polskiej

SPIS TREŚCI

ROZDZIAŁ I – POSTANOWIENIA OGÓLNE

§ 1
Podstawy prawne

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. *do uzupełnienia po publikacji ustawy*).
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).
3. Ustawa z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa (t.j.: Dz. U. z 2016 r, poz. 1725) – dalej: „Ustawa samorządowa".

§ 2

1. Polityka Bezpieczeństwa Informacji jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych w **Izbie Architektów Rzeczypospolitej Polskiej** oraz w **Okręgowych Izbach Architektów.** W przypadku określenia w Polityce obowiązków administratora jako IA RP, obowiązki te mają odpowiednie zastosowanie do Izb Okręgowych.
2. Ilekroć w niniejszym dokumencie będzie mowa o **IA RP** należy przez to rozumieć **Izbę Architektów Rzeczypospolitej Polskiej** reprezentowaną przez **Krajową Izbę Architektów RP** z siedzibą przy ul. Stawki 2A, 00-193 Warszawa oraz wchodzące w jej strukturę:
   a) Krajową Radę Izby Architektów
   b) Krajową Komisję Rewizyjną Izby Architektów
   c) Krajową Komisję Kwalifikacyjną Izby Architektów
   d) Krajowy Sąd Dyscyplinarny Izby Architektów
   e) Krajowego Rzecznika Odpowiedzialności Zawodowej
3. Za nadzór nad realizacją i przestrzeganiem Polityki oraz jej aktualizację odpowiada Izba Architektów Rzeczypospolitej Polskiej. Z zastrzeżeniem treści § 30 ust. 1, za nadzór nad aktualnością i wprowadzenie zmian w rejestrach, wykazach oraz wzorach dokumentów stanowiących załączniki do niniejszej Polityki odpowiada wyznaczony przez Krajową Radę IOD dla IA RP.

§ 3
Słownik pojęć stosowanych w niniejszej Polityce Bezpieczeństwa Informacji:

1. **Administrator Danych Osobowych** (**ADO**) - organ, jednostka organizacyjna, podmiot lub osoby decydujące o celach i środkach przetwarzania danych osobowych. W tym przypadku Administratorem Danych Osobowych jest **Izba Architektów Rzeczypospolitej Polskiej** reprezentowana przez **Prezesa Krajowej Rady Izby Architektów RP oraz Okręgowe Izby Architektów RP reprezentowane przez Przewodniczących.** W stosunku do zbiorów współadministrowanych z Izbami

Okręgowymi, Krajowa Izba Architektów Rzeczypospolitej Polskiej pełni funkcję głównej jednostki organizacyjnej dla przetwarzania prowadzonego w ramach współadministrowania zbiorami danych.

2. **Inspektor Ochrony Danych (IOD)**- osoba fizyczna wyznaczona przez Administratora Danych Osobowych, realizująca zadania opisane w art. 39 ust. 1 RODO. W odniesieniu do zbiorów danych współadministrowanych, zadania IOD wynikające z niniejszej Polityki pełni osoba wskazana przez właściwą Izbę Okręgową, która nie będzie miała formalnie statusu IOD. Postanowienia polityki stosuje się w takim przypadku odpowiednio. IOD oraz jego zastępcę powołuje Krajowa Rada. Osoby wskazane przez właściwe Izby Okręgowe współpracują z IOD oraz jego zastępcą.
3. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
4. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
5. **Działanie korygujące** - działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności, incydentu lub innej niepożądanej sytuacji.
6. **Działanie zapobiegawcze** - działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności, incydentu lub innej potencjalnej sytuacji niepożądanej.
7. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych.
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
9. **Identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
10. **Incydent** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego i zagrażają bezpieczeństwu informacji; naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
11. **Korekcja** - działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
12. **Kontrola (Audyt)** - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań polityk i procedur.
13. **Niezgodność** - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
14. **Nośniki danych** – dyskietki, płyty CD lub DVD, pamięć Flash, dyski twarde, taśmy magnetyczne lub inne urządzenia albo materiały służące do przechowywania plików z danymi.
15. **Odbiorca**– oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach

konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

16. **Podatność** - luka (słabość), która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę.
17. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
18. **Polityka Bezpieczeństwa Informacji (PBI)** – dokument o nazwie *Polityka Bezpieczeństwa Informacji Izby Architektów Rzeczypospolitej Polskiej.*
19. **Pracownik** – osoba fizyczna:
    a) świadcząca pracę na podstawie stosunku pracy, powołania, mianowania lub stosunku cywilnoprawnego,
    b) wykonująca zadania wyłącznie osobiście, w ramach prowadzonej działalności gospodarczej, powierzone jej na podstawie umowy cywilnoprawnej;.
    c) współpracująca w rozumieniu ustawy z dnia 13 października 1998 roku o systemie ubezpieczeń społecznych (Dz.U. 2016, poz. 963 z późn. zm.).
20. **Profilowanie** – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
21. **Przetwarzane danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
22. **Pseudonimizacja** - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
23. **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
24. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
25. **System tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.

26. **Serwisant** – firma lub pracownik firmy zajmujący się instalacją, naprawą i konserwacją sprzętu komputerowego.
27. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych.
28. **Słabość systemu** - zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu.
29. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
30. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. *do uzupełnienia po opublikowaniu ustawy*).
31. **Usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację (np. poprzez anonimizację danych), która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
32. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
33. **Użytkownik** - osoba upoważniona, która otrzymała uprawnienia do przetwarzania danych w systemie informatycznym. Użytkownik posiada indywidualny identyfikator oraz hasło do systemu i działa w granicach polecenia administratora lub podmiotu przetwarzającego.
34. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
35. **Zagrożenie** - potencjalna możliwość wystąpienia incydentu.
36. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
37. **Zdarzenie** - błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z zagrożeniem bezpieczeństwa danych osobowych.

§ 4

1. Polityka Bezpieczeństwa Informacji określa:
   a) granice dopuszczalnego zachowania Użytkowników systemu informatycznego oraz wskazuje konsekwencje w stosunku do osób naruszających zasady ochrony danych osobowych,
   b) prawa i obowiązki Użytkowników systemu informatycznego w zakresie ochrony danych osobowych przetwarzanych w tym systemie,
   c) sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę tych danych,
   d) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
   e) wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych,
   f) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych;
   g) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
   h) rejestr czynności przetwarzania danych osobowych,
   i) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych,

j) sposób realizacji żądań osób uprawnionych, których dane są przechowywane.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   a) **poufność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom,
   b) **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   c) **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   d) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej,
   e) **dostępność informacji** - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   f) **zarządzanie ryzykiem** - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych służących do przetwarzania danych osobowych.

3. Niniejszy dokument został wprowadzony Uchwałą Krajowej Rady Izby Architektów RP oraz udostępniony wszystkim Użytkownikom systemu oraz pozostałym pracownikom posiadającym dostęp do przetwarzanych danych osobowych.
4. Niniejszy dokument jest rekomendowany do przyjęcia przez Izby Okręgowe. Przyjęcie dokumentu powinno nastąpić w drodze uchwały Okręgowej Rady.
5. Każda osoba, mająca dostęp do danych osobowych jest zobowiązana do zapoznania się z niniejszym dokumentem oraz potwierdzenia tego faktu poprzez złożenie pisemnego oświadczenia włączanego do akt osobowych. **Wzór oświadczenia** stanowi ***załącznik nr 4*** do Zarządzenia.

RODZIAŁ II – ZASADY PRZETWARZANIA DANYCH OSOBOWYCH. POWIERZENIE. UDOSTĘPNIANIE. ODPOWIEDZIALNOŚĆ. ZABEZPIECZENIA. OBOWIĄZEK INFORMACYJNY

§ 5
Zasady ogólne przetwarzania danych osobowych

1. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. IA RP może żądać podania jedynie tych danych, które są niezbędne do realizacji celów i zadań Izby oraz tych danych, do przetwarzania których upoważniona została zgodnie z powszechnie obowiązującymi przepisami prawa, a w szczególności z Ustawą samorządową.
2. Zakres danych osobowych przetwarzanych przez jednego Użytkownika w systemie informatycznym nie może być szerszy niż powierzony do przetwarzania w związku z wykonywanymi przez niego obowiązkami.
3. Okres przechowywania poszczególnych kategorii dokumentów zawierających dane osobowe określa ***załącznik nr 11***. Po upływie okresów tam wskazanych, dane osobowe powinny zostać usunięte lub zanonimizowane (tj. przechowywane w postaci uniemożliwiającej powiazanie tych danych z konkretną osobą fizyczną).

§ 6

Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia lub części pomieszczeń w siedzibach IA RP zgodnie z treścią ***załącznika nr 1***.

§ 7

Wymagany przez RODO rejestr czynności przetwarzania stanowi ***załącznik nr 2*** *do Polityki.*

§ 8

1. Wszystkie osoby, które przetwarzają dane osobowe w imieniu administratora, w tym pracownicy i zleceniobiorcy (tzw. personel administratora) muszą posiadać pisemne **upoważnienie do przetwarzania danych oraz polecenie przetwarzania danych** nadane przez ADO. Dodatkowo, w uzasadnionych przypadkach ADO może przed upoważnieniem danej osoby do dostępu do zbioru danych zażądać podpisania **oświadczenia o zachowaniu poufności** tych danych. Wzór upoważnienia stanowi ***załącznik nr 3*** do Polityki. Wzór oświadczenia o zachowaniu poufności stanowi ***załącznik nr 4*** do Polityki. Polecenie przetwarzania danych może być wydane w dowolnie udokumentowanej formie przez ADO lub przełożonego osoby upoważnionej do przetwarzania danych osobowych (np. w formie maila lub pisemnego polecenia służbowego).
2. Warunkiem dostępu do zbioru danych osobowych podmiotów zewnętrznych (np. zewnętrznych firm i instytucji) jest podpisanie przez te podmioty umowy o powierzeniu danych, stanowiącej ***załącznik nr 10***, której minimalny zakres zgodny będzie z art. 28 ust. 3 RODO. Zasady powierzania danych osobowych określone zostały w § 11.

§ 9

1. Upoważnienia do przetwarzania danych osobowych w systemie informatycznym wydawane są zgodnie z właściwą procedurą określoną w niniejszym dokumencie. Upoważnienia, o których mowa w ust. 1 niniejszego paragrafu, ważne są do dnia odwołania lub do chwili ustania zatrudnienia upoważnionego pracownika.
2. ADO może upoważnić IOD/jego zastępcę do zarządzania nadawaniem, odbieraniem lub modyfikowaniem uprawnień do określonych zbiorów danych.

§ 10

1. W zbiorach danych gromadzonych w systemie informatycznym zabrania się przetwarzania danych ujawniających:
   a) stan zdrowia,
   b) pochodzenie rasowe lub etniczne,
   c) poglądy polityczne,
   d) przekonania religijne lub filozoficzne,
   e) przynależność wyznaniową,
   f) przynależność partyjną lub związkową,
   g) dane genetyczne,
   h) dane biometryczne,

i) nałogi,
j) preferencje seksualne,

chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę.

2. **Dane o skazaniach, w tym dane o niekaralności** można przetwarzać wyłącznie w sytuacjach określonych przepisami prawa.
3. Do **profilowania** zabrania się używania danych wymienionych w ust. 1 niniejszego paragrafu, chyba, że wymagają tego obowiązujące przepisy prawa, osoba, której dane dotyczą wyraziła na to zgodę lub jest to podyktowane ważnym interesem publicznym.
4. Przy profilowaniu Administrator Danych Osobowych obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.
5. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą.
6. Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie przez IA RP jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

§ 11

Powierzenie przetwarzania danych osobowych

1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy IA RP oraz pracownicy podmiotów (procesorów) świadczących usługi na jego rzecz w związku z realizacją celów i zadań administratora. W odniesieniu do zbiorów współadministrowanych niniejsze postanowienie stosuje się odpowiednio do części zbioru, współadministrowanego przez Izbę Okręgową.
2. Powierzenie przetwarzania danych osobowych następuje na podstawie **umowy powierzenia przetwarzania danych osobowych** lub **innego aktu (instrumentu) prawnego,** zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej w postaci oświadczenia złożonego za pośrednictwem poczty e-mail, określonej opcji internetowej lub zapisanego na elektronicznym nośniku informacji. Przykładowy wzór umowy powierzenia stanowi ***załącznik nr 10*** do Polityki.
3. Okres powierzenia oraz zakres danych osobowych powierzanych powinien być adekwatny do celu powierzenia.
4. Administrator danych osobowych zobowiązany jest do dokumentowania powierzania tych danych w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi (***załącznik nr 6*** do Polityki).
5. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (**podpowierzenie danych**), wymagana jest szczegółowa lub ogólna zgoda ADO na przekazanie powierzonych danych, wyrażona w formie pisemnej lub formie elektronicznej.

§ 12

Udostępnianie danych osobowych

1. **Udostępnienie danych osobowych podmiotowi zewnętrznemu** może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz

administrator danych pozyskujący dane drogą udostępnienia posiadają do tego odpowiednią podstawę prawną.
2. ADO może **odmówić udostępnienia** danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie praw i wolności osób, których dane dotyczą lub innych osób oraz w sytuacji, w której udostępnienie danych nie znajduje uzasadnienia w podstawach prawnych wskazanych przez wnioskującego o udostępnienie danych.
3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać pseudonimizacji tych danych.
4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 13

Zabezpieczenia danych osobowych

W celu zapewnienia należytej ochrony przetwarzania danych osobowych, w IA RP zastosowano środki zabezpieczające powierzone zbiory danych w postaci **zabezpieczeń technicznych i organizacyjnych** wymienionych poniżej:

Zabezpieczenia techniczne

1. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz lub w szafach zamykanych na klucz.
2. Pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy.
3. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce lub protokolarne przekazanie dokumentów do zniszczenia wyspecjalizowanej firmie zewnętrznej.
4. Zastosowano urządzenia typu UPS, generator prądu lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
5. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła lub zabezpieczeń biometrycznych.
6. W przypadku wystąpienia konieczności dostępu do zbioru danych osobowych w czasie nieobecności pracownika upoważnionego do przetwarzania danych w tym zbiorze, właściwy ADO lub IOD może udostępnić ten zbiór innemu pracownikowi w celu dokonania niezbędnych czynności służbowych. Po powrocie nieobecny pracownik otrzymuje nowe indywidualne hasło dostępu.
7. Dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (np. Word), arkuszach kalkulacyjnych (np. Excel) i innych programach do tworzenia baz danych oraz w systemach informatycznych, np. Płatnik, system bankowości elektronicznej itp. zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie itp.

8. Do ochrony dostępu do sieci komputerowej użyto systemu typu Firewall.
9. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
10. Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych.
11. Dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora (loginu) Użytkownika oraz hasła.

Zabezpieczenia organizacyjne

1. Opracowano i wdrożono Politykę Bezpieczeństwa Informacji obejmującą między innymi zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Izbie Architektów Rzeczypospolitej Polskiej.
2. W IA RP powołano Inspektora Ochrony Danych oraz jego zastępcę, który sprawuje nadzór nad przetwarzaniem danych osobowych.
3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie, o którym mowa w § 8 niniejszego dokumentu albo podpisały umowę o powierzeniu danych, działające na polecenie ADO.
4. Prowadzone są wykazy osób i podmiotów opisane w § 17 ust. 4 niniejszego dokumentu. Za prowadzenie wykazów odpowiada IOD/jego zastępca, z zastrzeżeniem § 30 ust. 1.
5. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
6. Wszyscy Użytkownicy systemu informatycznego zostali przeszkoleni w zakresie zabezpieczeń tego systemu.
7. Wykonane kopie zapasowe zbiorów danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

§ 14

Odpowiedzialność

1. Nieprzestrzeganie zasad ochrony danych osobowych może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych z wynikającymi z tego konsekwencjami. W określonych przepisami Ustawy o ochronie danych osobowych (art. 107 i 108) za naruszenie zasad przetwarzania danych osobowych może grozić odpowiedzialność karna.
2. Odpowiedzialności dyscyplinarnej podlega każdy pracownik, który:
   a) przetwarza w zbiorze danych dane osobowe, do których nie jest upoważniony,
   b) przetwarza w zbiorze danych dane, których przetwarzanie jest zabronione,
   c) przetwarza w zbiorze danych dane niezgodne z celem stworzenia tego lub innych zbiorów,
   d) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
   e) nie zgłasza zbiorów danych podlegających rejestracji,
   f) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,

g) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw,
h) nie poinformuje IOD o Incydentach bądź innych zdarzenia, stanowiących naruszenie zasad ochrony danych osobowych,
i) w inny sposób narusza przepisy bądź wewnętrzne dokumenty (w tym niniejszą Politykę) opisujące zasady ochrony danych osobowych.

§ 15

Obowiązek informacyjny

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany poinformować tę osobę o zasadach przetwarzania danych osobowych w zakresie odpowiadającym treści art. 13 RODO lub art. 14 RODO w przypadku pozyskania danych w sposób inny niż od osoby, której dane dotyczą, poprzez przekazanie do wiadomości tej osoby odpowiedniej Polityki prywatności.
2. Obowiązek poinformowania wymieniony w ust 1 niniejszego paragrafu powinien być wykonany w momencie pozyskiwania danych z wyjątkiem sytuacji, w której:
   a) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
   b) osoba, której dane dotyczą, posiada już informacje, których udzielenia wymaga art. 13 RODO.
3. Obowiązek poinformowania wymieniony w ust. 2 niniejszego paragrafu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie z wyjątkiem sytuacji opisanych w art. 25 ust. 2 ustawy.

ROZDZIAŁ III – INSPEKTOR OCHRONY DANYCH (IOD)

§ 16

1. Inspektor Ochrony Danych (IOD) to osoba fizyczna powołana przez Administratora Danych Osobowych, zgodnie z art. 39 RODO zobowiązana do:
   a) informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
   b) monitorowania przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
   c) udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z art. 35 RODO,
   d) współpracy z organem nadzorczym,
   e) pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych

przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Administrator Danych Osobowych jest zobowiązany do zgłoszenia powołania (lub odwołania) IOD do rejestracji PUODO wyłącznie przy użyciu formularzy zgłoszeń powołania i odwołania IOD. W przypadku niepowołania IOD, funkcje mu przypisane pełni ADO w zakresie zgodnym z obowiązującymi przepisami.

§ 17

1. IOD prowadzi rejestr czynności przetwarzania danych oraz, kiedy jest to wymagane, przeprowadza ocenę skutków dla ochrony danych zgodnie z art. 35 RODO.
2. IOD jest również zobowiązany do przeprowadzania **analizy ryzyk** związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym.
3. IOD bierze udział w prowadzonych w IA RP projektach, odpowiadając za ich zgodność z zasadami ochrony danych osobowych na etapie projektowania („privacy by design").
4. Ponadto IOD prowadzi następujące wykazy:
   a) wykaz osób, którym nadano upoważnienia do przetwarzania danych osobowych (***załącznik nr 5*** do Polityki),
   b) wykaz podmiotów, którym powierzono dane osobowe do przetwarzania (***załącznik nr 6*** do Polityki).

ROZDZIAŁ IV – OGÓLNE WARUNKI KORZYSTANIA Z SYSTEMU INFORMATYCZNEGO

§ 18

1. Korzystanie z funkcjonalności systemu informatycznego jest możliwe pod warunkiem złożenia do IOD wniosku o nadanie, zmianę lub wycofanie dostępu dla osoby uprawnionej. Wniosek może mieć formę wiadomości e-mail.
2. Po weryfikacji wniosku przez IOD, Użytkownikowi zostaje wydane upoważnienie do przetwarzania danych osobowych w zbiorach administrowanych w systemie informatycznym stosowanym w IA RP.

§ 19

1. Zgodnie z postanowieniami niniejszej Polityki, zabrania się Użytkownikowi systemu podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń systemu.
2. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom.
3. Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika.

4. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
5. Użytkownik zobowiązany jest do przestrzegania zasady czystego biurka, w szczególności przed opuszczeniem swego stanowiska pracy Użytkownik powinien schować wszelkie dokumenty związane z używanym systemem oraz informatyczne nośniki danych (dyskietki, płyty CD, DVD, BD, pendrive itp.).

§ 20

Każdy Użytkownik jest zobowiązany do zapoznania się i zaakceptowania zasad korzystania z systemu informatycznego.

ROZDZIAŁ V - POCZTA ELEKTRONICZNA, INTERNET

§ 21

1. W systemie informatycznym wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w systemie.
2. Użytkownik zobowiązany jest do dbania o bezpieczeństwo konta mailowego, o którym mowa powyżej, w szczególności do:
   a) używania silnego hasła dostępu,
   b) nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł,
   c) zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.
3. Użytkownik zobowiązany jest do korzystania z sieci Internet w sposób, który nie zagraża bezpieczeństwu danych gromadzonych i przetwarzanych w systemie.

ROZDZIAŁ VI – POSTĘPOWANIE NA WYPADEK ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 22

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) próby naruszenia ochrony danych:
      - z zewnątrz - włamania do systemu, podsłuch, kradzież danych
      - z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych
   b) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne,
   c) awarie sprzętu lub uszkodzenie oprogramowania,
   d) zabór sprzętu lub nośników z ważnymi danymi,
   e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
   f) usiłowanie zakłócenia działania systemu informatycznego.
2. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

b) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka lub ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
d) zdarzenia losowe zewnętrzne (pożar obiektu albo pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
e) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych),
f) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:
   a) zgłoszenia od Użytkowników,
   b) alarmy z systemów informatycznych,
   c) analizy incydentów,
   d) wyniki audytów lub kontroli.

§ 23

Każdy pracownik, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Inspektora Ochrony Danych. Zasady działania w takich przypadkach określa **tabela nr 1**

Tabela nr 1. Zasady działania w przypadku zagrożenia lub naruszenia ochrony danych osobowych

Kod uchybienia lub zagrożenia	Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru	Należy zabezpieczyć dane osobowe oraz powiadomić IOD, który rejestruje incydent
2	Komputer nie jest zabezpieczony hasłem	Należy zabezpieczyć dane osobowe oraz powiadomić IOD, który rejestruje incydent
3	Dostęp do danych mają osoby nieupoważnione	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który sporządza protokół incydentu
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Należy powiadomić IOD, który powinien sprawdzić system uwierzytelniania oraz sprawdzić, czy nie doszło do kradzieży lub zniszczenia danych. IOD protokołuje incydent
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Należy nie dopuścić do kradzieży danych i powiadomić IOD. IOD powinien zabezpieczyć nośnik danych sporządzić protokół incydentu
6	Próba kradzieży danych osobowych w formie papierowej	Należy nie dopuścić do kradzieży danych osobowych i powiadomić IOD. IOD powinien zabezpieczyć dane i powiadomić ADO. IOD sporządza protokół incydentu
7	Nieuprawniony dostęp do danych osobowych w formie papierowej	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który sporządza protokół incydentu
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Należy powiadomić IOD, który powinien zabezpieczyć pomieszczenie i zarejestrować incydent
9	Próba włamania do pomieszczenia/budynku	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD sporządza protokół incydentu

10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych oraz firewall IOD powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół incydentu oraz poinformować PUODO ewentualnie – jeżeli zagrożone są prawa i wolności podmiotów danych – informuje również osoby, których naruszenie dotyczy albo zarejestrować incydent, jeżeli nie doszło do utraty danych osobowych
11	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić IOD. IOD powinien zaktualizować lub nabyć oprogramowanie antywirusowe. IOD sporządza protokół incydentu
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. IOD sporządza protokół incydentu oraz PUODO ewentualnie – jeżeli zagrożone są prawa i wolności podmiotów danych – informuje również osoby, których naruszenie dotyczy
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. IOD sporządza Protokół zagrożenia oraz informuje PUODO ewentualnie – jeżeli zagrożone są prawa i wolności podmiotów danych – informuje również osoby, których naruszenie dotyczy
14	Uszkodzenie komputerów, nośników danych	Należy powiadomić IOD, który powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. IOD powiadamia ADO i sporządza Protokół incydentu. Jeżeli utrata danych ma charakter nieodwracalny, IOD informuje PUODO ewentualnie – jeżeli zagrożone są prawa i wolności podmiotów danych – informuje również osoby, których naruszenie dotyczy
15	Próba nieprawidłowej interwencji przy sprzęcie komputerowym	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić IOD, który rejestruje incydent
16	Zdarzenia losowe	Należy oszacować powstałe straty i poinformować IOD, który w zależności od konsekwencji wywołanych przez zdarzenie losowe – rejestruje incydent albo sporządza Protokół incydentu oraz informuje PUODO ewentualnie – jeżeli zagrożone są prawa i wolności podmiotów danych – informuje również osoby, których naruszenie dotyczy

§ 24

W przypadku stwierdzenia **wystąpienia zagrożenia**, IOD prowadzi postępowanie wyjaśniające, w toku którego:

a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
b) inicjuje ewentualne działania dyscyplinarne,
c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
d) dokumentuje prowadzone postępowania,
e) odnotowuje zdarzenie w rejestrze incydentów, zgodnie z ***załącznikiem 7*** do Polityki.

§ 25

W przypadku **stwierdzenia incydentu** (naruszenia) IOD prowadzi postępowanie wyjaśniające, w toku którego:

a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
b) ustala osoby odpowiedzialne za naruszenie,
c) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,

d) dokumentuje prowadzone postępowania,
e) w terminie nie dłuższym niż 72 godziny od potwierdzenia wystąpienia Incydentu IOD informuje o wystąpieniu incydentu PUODO,
f) W przypadku, gdy Incydent może w konsekwencji spowodować zagrożenie dla praw i wolności osób, których danych Incydent dotyczył IOD w miarę możliwości informuje te osoby niezwłocznie o wystąpieniu incydentu i jego potencjalnych skutkach.

§ 26

IOD jest odpowiedzialny za **analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabości systemu** ochrony danych osobowych. Gdy stwierdzi konieczność **podjęcia działań korygujących** lub zapobiegawczych, określa źródło powstania incydentu, zagrożenia lub słabości, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną.

§ 27

IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

§ 28

Integralną częścią *Polityki Bezpieczeństwa Informacji* są nw. dokumenty prowadzone przez IOD w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych:
a) Rejestr incydentów – ***załącznik nr 7*** do niniejszej Polityki,
b) Protokół incydentu – ***załącznik nr 8*** do niniejszej Polityki.

ROZDZIAŁ VII REALIZACJA ŻĄDAŃ OSÓB UPRAWNIONYCH

§ 29

1. Osoby uprawnione mogą złożyć następujące dyspozycje w zakresie przetwarzania ich danych osobowych:
a) udzielenia informacji w zakresie przetwarzania danych osobowych,
b) przeniesienia danych osobowych,
c) ograniczenia zakresu przetwarzania, np. poprzez wyłączenie niektórych celów przetwarzania,
d) żądanie zaprzestania profilowania danych osobowych,
e) żądanie zaprzestania podejmowania zautomatyzowanych decyzji opartych na profilowaniu,
f) żądanie zaprzestania przetwarzania danych osobowych (realizacja „prawa do bycia zapomnianym"),
2. W przypadku złożenia zapytania o potwierdzenie przetwarzania danych osobowych (np. imienia, nazwiska, numeru telefonu, adresu e-mail) przez jakąkolwiek osobę fizyczną, IOD lub inna osoba wyznaczona przez ADO udziela informacji, czy dane są przetwarzane, a w przypadku odpowiedzi pozytywnej, odpowiedź jest uzupełniona o następujące informacje:
a) od kiedy dane są przetwarzane,

b) do jakich kategorii zalicza się dane osobowe,
c) jaka jest podstawa przetwarzania (np. zgoda lub realizacja obowiązku prawnego) ewentualnie informacje o źródle danych – jeżeli dane nie zostały zebrane od osoby, której one dotyczą,
d) w jakich celach dane są przetwarzane,
e) w jakiej roli występuje IA RP (administrator, podmiot przetwarzający czy odbiorca),
f) do kiedy dane będą przetwarzane,
g) czy dane podlegają profilowaniu a jeżeli tak – to w jakich celach,
h) czy dane zostały udostępnione do odbiorców znajdujących się w państwach trzecich lub organizacjach międzynarodowych,
i) odnośnik do odpowiedniej polityki prywatności,
j) informację o prawie wniesienia skargi do organu nadzoru.

3. W razie wątpliwości, IOD/jego zastępca ma prawo uzależnić udzielenie informacji od przekazania informacji, które w sposób jednoznaczny potwierdzą, że pytający jest rzeczywiście osobą, której dane są przetwarzane (np. poprzez przesłanie kopii umowy lub weryfikację dodatkowych informacji).
4. W przypadku, gdy zapytania od tej samej osoby lub osób reprezentujących tą samą grupę (np. przedstawicieli jednej firmy) powtarzają się w sposób uporczywy, ADO ma możliwość udzielenia kolejnej informacji od złożenia opłaty, odpowiadającej kosztom udzielenia informacji – a w szczególności kosztom pracy osoby, delegowanej do udzielenia informacji.
5. W przypadku żądania przeniesienia danych osobowych, ADO realizuje tą dyspozycję, o ile posiada środki techniczne i przeniesienie danych jest możliwe, zaś wskazany odbiorca danych potwierdzi gotowość do przyjęcia danych oraz wskaże sposób migracji (platformę informatyczną do przekazania danych). Postanowienia ust. 3 oraz ust. 4 powyżej stosuje się odpowiednio.
6. W przypadku otrzymania dyspozycji ograniczenia przetwarzania danych, zaprzestania profilowania danych osobowych lub zaprzestania podejmowania zautomatyzowanych decyzji opartych o profilowanie, ADO realizuje tą dyspozycję nie później niż w ciągu 5 dni roboczych od dnia jej otrzymania. Ust. 3 stosuje się odpowiednio.
7. W przypadku otrzymania żądania zaprzestania przetwarzania danych osobowych, ADO po weryfikacji, czy i w jakim zakresie żądanie powinno być zrealizowane, wykreśla dane osobowe ze wszystkich zbiorów danych, pozostawiając jedynie informacje niezbędne do ochrony przed roszczeniami – tj. dane o sposobie i dacie pozyskania danych osobowych, zakresie przetwarzania, podstawie przetwarzania i dacie otrzymania oraz realizacji dyspozycji usunięcia danych. Dane takie przechowywane są przez okres do 11 lat po dacie otrzymania dyspozycji usunięcia danych w celach ewentualnej ochrony interesów prawnych IA RP. ADO informuje podmiot żądający usunięcia o zrealizowaniu żądania lub przyczynie odmowy jego realizacji.
8. Wzór rejestru realizacji czynności Osób uprawnionych stanowi ***załącznik nr 9*** do Polityki.
9. W ramach realizacji prawa do bycia zapomnianym, Administrator informuje wszystkich przetwarzających, odbiorców oraz strony trzecie o konieczności usunięcia danych osobowych ze zbiorów, które te dane zawierają.
10. Realizacja prawa do bycia zapomnianym następuje w terminie 10 dni roboczych od momentu złożenia takiej dyspozycji przez osobę Uprawnioną. Ust. 3 stosuje się odpowiednio.
11. O wszelkich zmianach w zakresie danych osobowych (w tym o wykreśleniu, skorygowaniu, ograniczeniu celu przetwarzania, zaprzestaniu profilowania) Osoba,

której zmiana ta dotyczy informowana jest poprzez kontakt mailowy lub telefoniczny – jeżeli Administrator nie dysponuje jej adresem mailowym. W przypadku realizacji „prawa do bycia zapomnianym" Administrator informuje również o przekazaniu dyspozycji o wykreśleniu danych do podmiotów, którym dane te zostały przekazane lub powierzone.

ROZDZIAŁ VIII – POSTANOWIENIA KOŃCOWE

§ 30

1. Następująca dokumentacja dotycząca ochrony danych osobowych prowadzona jest samodzielnie przez każdą z Izb Okręgowych przez osobę wyznaczoną w ramach Izby Okręgowej:

a) Wykaz pomieszczeń, w których przetwarzane są dane osobowe (obszar)
b) Rejestr czynności przetwarzania danych;
c) Wykaz osób upoważnionych do przetwarzania danych osobowych;
d) Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych;
e) Wykaz udostępnień danych osobowych osobom, których dane dotyczą;
f) Rejestr incydentów;
g) Protokół incydentu;
h) Umowa powierzenia przetwarzania danych osobowych.

2. IOD/jego zastępca wyznaczony przez Krajową Radę IA RP uprawniony jest do dokonywania weryfikacji oraz audytów w zakresie prawidłowości w zakresie przetwarzania danych osobowych przez każdą z Izb Okręgowych i uprawniony jest do wydawania władzom danej Izby Okręgowej wytycznych w tym zakresie.

3. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz RODO.

Niniejszy dokument wchodzi w życie z dniem .....

.....
(Administrator Danych Osobowych)